Phishing Attacks

Phishing Attacks

What is it and how to avoid it ?

Phishing Attacks

A phishing attack is when a malicious person pretends to be someone you trust, like a friend or a company, to trick you.

They might send fake emails or messages that look real to get you to share your passwords or personal info.

The goal is to steal your information or trick you into doing something that helps them.

Phishing Attacks

franck.ridel.14 - Vous avez (1) colis en attente de livraison. 📦✔ Spam ×

Chronopost 📦 <info@msnkwnwl.spectraldiscoveries.it.com> (sent by Chronopost.fr)
to me

Tue, Jun 17, 8:13 PM (2 days ago)

Why is this message in spam? It seems to be an auto-reply to a message that pretended to be sent from your email address.

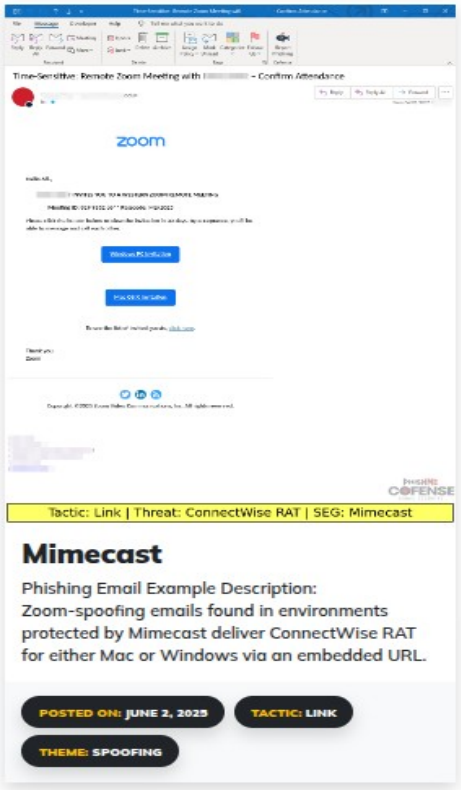
Report not spam | Report phishing

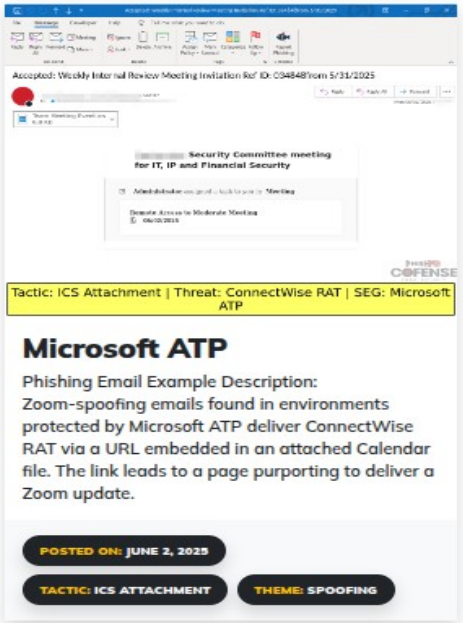
Action requise : Livraison d'un colis en attente
Chronopost
N° : CHR19220609FR
Code de suivi
Cher client, franck.ridel.14
Vous avez (1) colis en attente de livraison
Confirmez vos informations d'expédition
■ Statut : Retenu au centre de distribution (en attente de dédouanement).
Des frais de livraison peuvent s'appliquer.
Planifier la livraison maintenant

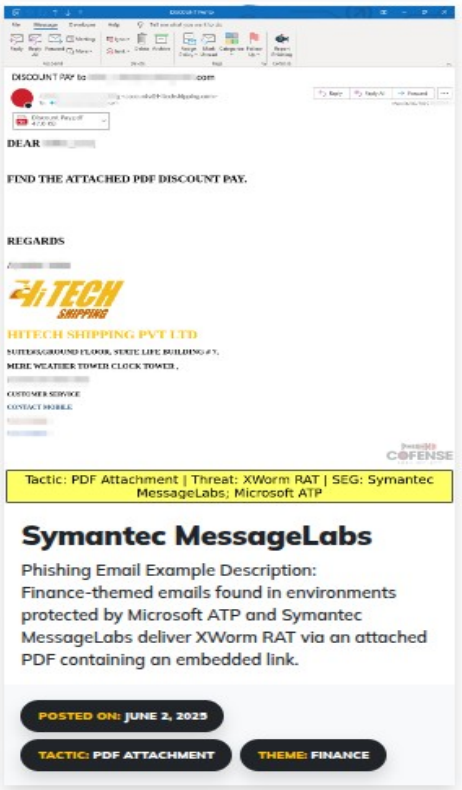
Phishing Attacks

Real examples

https://cofense.com/knowledge-center-hub/real-phishing-email-examples


Tactic: Link | Threat: ConnectWise RAT | SEG: Mimecast
Mimecast
Phishing Email Example Description:
Zoom-spoofing emails found in environments protected by Mimecast deliver ConnectWise RAT for either Mac or Windows via an embedded URL.
POSTED ON: JUNE 2, 2025
TACTIC: LINK
THEME: SPOOFING

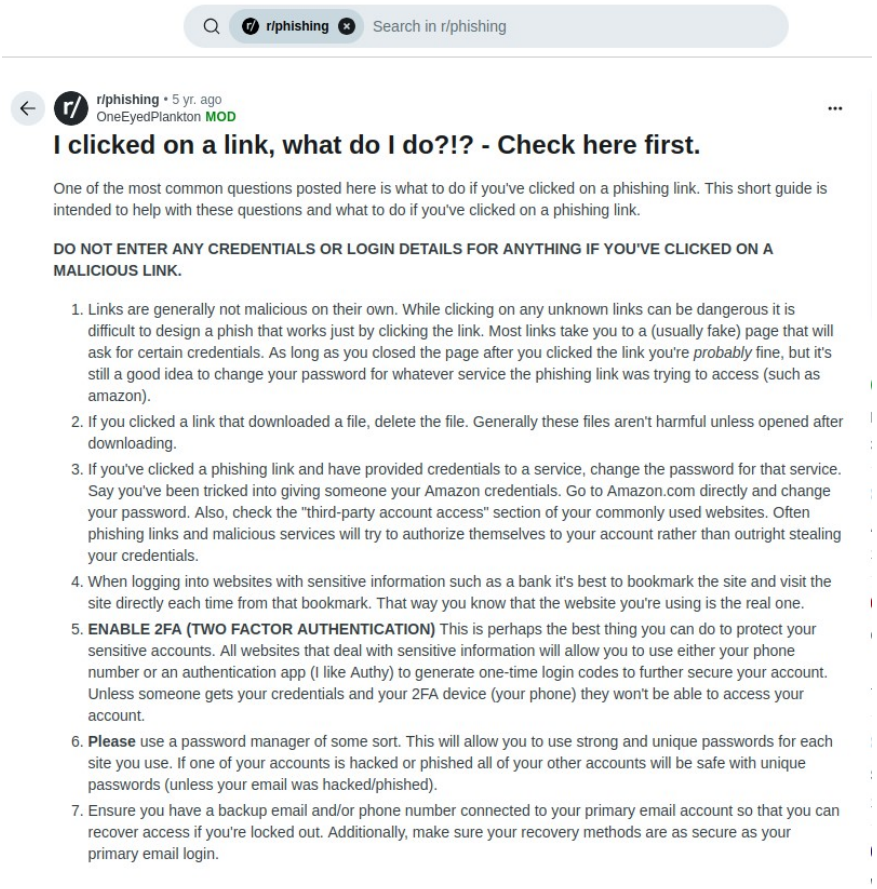

Tactic: ICS Attachment | Threat: ConnectWise RAT | SEG: Microsoft ATP
Microsoft ATP
Phishing Email Example Description:
Zoom-spoofing emails found in environments protected by Microsoft ATP deliver ConnectWise RAT via a URL embedded in an attached Calendar file. The link leads to a page purporting to deliver a Zoom update.
POSTED ON: JUNE 2, 2025
TACTIC: ICS ATTACHMENT
THEME: SPOOFING


DEAR
FIND THE ATTACHED PDF DISCOUNT PAY.
REGARDS
HITECH SHIPPING PVT LTD
Tactic: PDF Attachment | Threat: XWorm RAT | SEG: Symantec MessageLabs; Microsoft ATP
Symantec MessageLabs
Phishing Email Example Description:
Finance-themed emails found in environments protected by Microsoft ATP and Symantec MessageLabs deliver XWorm RAT via an attached PDF containing an embedded link.
POSTED ON: JUNE 2, 2025
TACTIC: PDF ATTACHMENT
THEME: FINANCE

Phishing Attacks

First aid

https://www.reddit.com/r/phishing/comments/jgt53p/i_clicked_on_a_link_what_do_i_do_check_here_first/



r/phishing Search in r/phishing

r/phishing • 5 yr. ago
OneEyedPlankton MOD

I clicked on a link, what do I do?!? - Check here first.

One of the most common questions posted here is what to do if you've clicked on a phishing link. This short guide is intended to help with these questions and what to do if you've clicked on a phishing link.

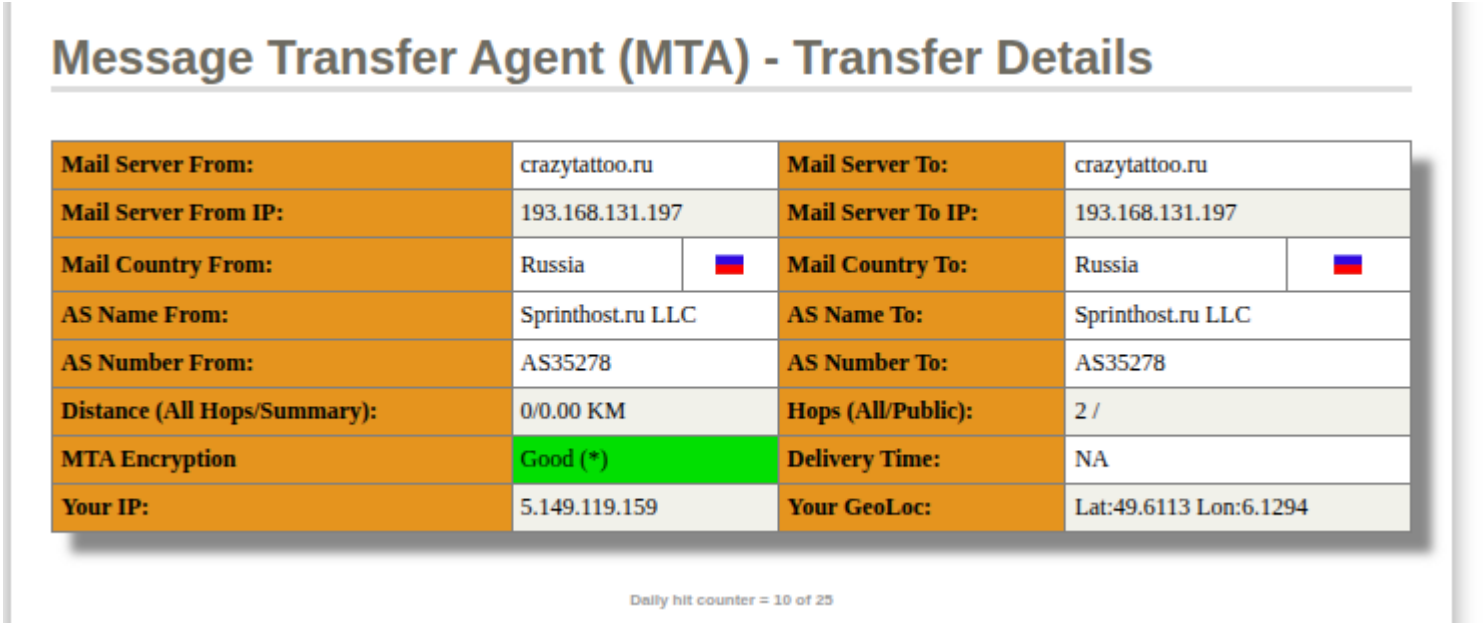
DO NOT ENTER ANY CREDENTIALS OR LOGIN DETAILS FOR ANYTHING IF YOU'VE CLICKED ON A MALICIOUS LINK.

1. Links are generally not malicious on their own. While clicking on any unknown links can be dangerous it is difficult to design a phish that works just by clicking the link. Most links take you to a (usually fake) page that will ask for certain credentials. As long as you closed the page after you clicked the link you're *probably* fine, but it's still a good idea to change your password for whatever service the phishing link was trying to access (such as amazon).
2. If you clicked a link that downloaded a file, delete the file. Generally these files aren't harmful unless opened after downloading.
3. If you've clicked a phishing link and have provided credentials to a service, change the password for that service. Say you've been tricked into giving someone your Amazon credentials. Go to Amazon.com directly and change your password. Also, check the "third-party account access" section of your commonly used websites. Often phishing links and malicious services will try to authorize themselves to your account rather than outright stealing your credentials.
4. When logging into websites with sensitive information such as a bank it's best to bookmark the site and visit the site directly each time from that bookmark. That way you know that the website you're using is the real one.
5. **ENABLE 2FA (TWO FACTOR AUTHENTICATION)** This is perhaps the best thing you can do to protect your sensitive accounts. All websites that deal with sensitive information will allow you to use either your phone number or an authentication app (I like Authy) to generate one-time login codes to further secure your account. Unless someone gets your credentials and your 2FA device (your phone) they won't be able to access your account.
6. **Please** use a password manager of some sort. This will allow you to use strong and unique passwords for each site you use. If one of your accounts is hacked or phished all of your other accounts will be safe with unique passwords (unless your email was hacked/phished).
7. Ensure you have a backup email and/or phone number connected to your primary email account so that you can recover access if you're locked out. Additionally, make sure your recovery methods are as secure as your primary email login.

Suspicious Email Analysis

Email Header Analysis

- https://mailheader.org/



Message Transfer Agent (MTA) - Transfer Details

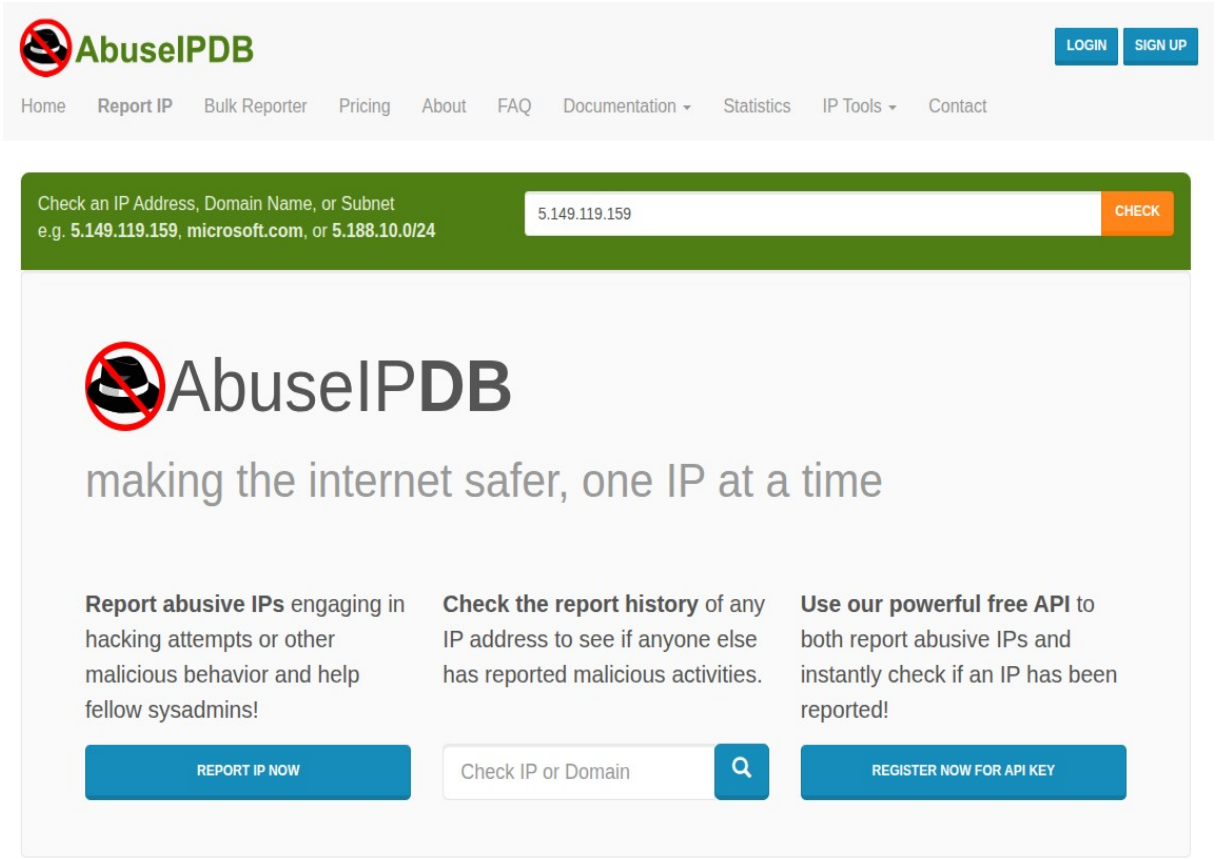
Mail Server From:	crazytattoo.ru	**Mail Server To:**	crazytattoo.ru
Mail Server From IP:	193.168.131.197	**Mail Server To IP:**	193.168.131.197
Mail Country From:	Russia	**Mail Country To:**	Russia
AS Name From:	Sprinthost.ru LLC	**AS Name To:**	Sprinthost.ru LLC
AS Number From:	AS35278	**AS Number To:**	AS35278
Distance (All Hops/Summary):	0/0.00 KM	**Hops (All/Public):**	2 /
MTA Encryption	Good (*)	**Delivery Time:**	NA
Your IP:	5.149.119.159	**Your GeoLoc:**	Lat:49.6113 Lon:6.1294

Daily hit counter = 10 of 25

Suspicious Email Analysis

URL and IP Reputation Analysis

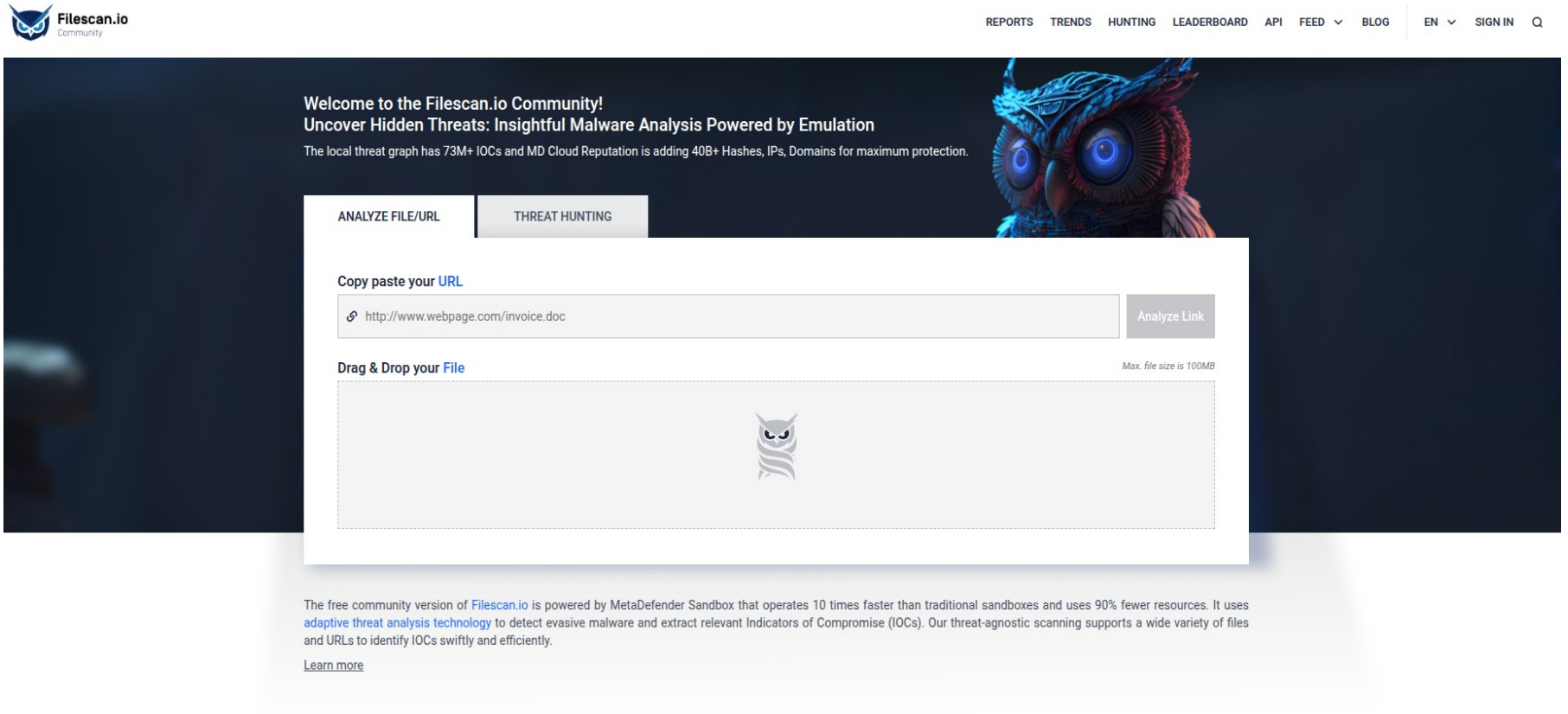
- https://www.abuseipdb.com/


AbuseIPDB
LOGIN
SIGN UP
Home
Report IP
Bulk Reporter
Pricing
About
FAQ
Documentation
Statistics
IP Tools
Contact
Check an IP Address, Domain Name, or Subnet
e.g. 5.149.119.159, microsoft.com, or 5.188.10.0/24
5.149.119.159
CHECK
AbuseIPDB
making the internet safer, one IP at a time
Report abusive IPs engaging in hacking attempts or other malicious behavior and help fellow sysadmins!
Check the report history of any IP address to see if anyone else has reported malicious activities.
Use our powerful free API to both report abusive IPs and instantly check if an IP has been reported!
REPORT IP NOW
Check IP or Domain
REGISTER NOW FOR API KEY

Suspicious Email Analysis

File and Malware Analysis

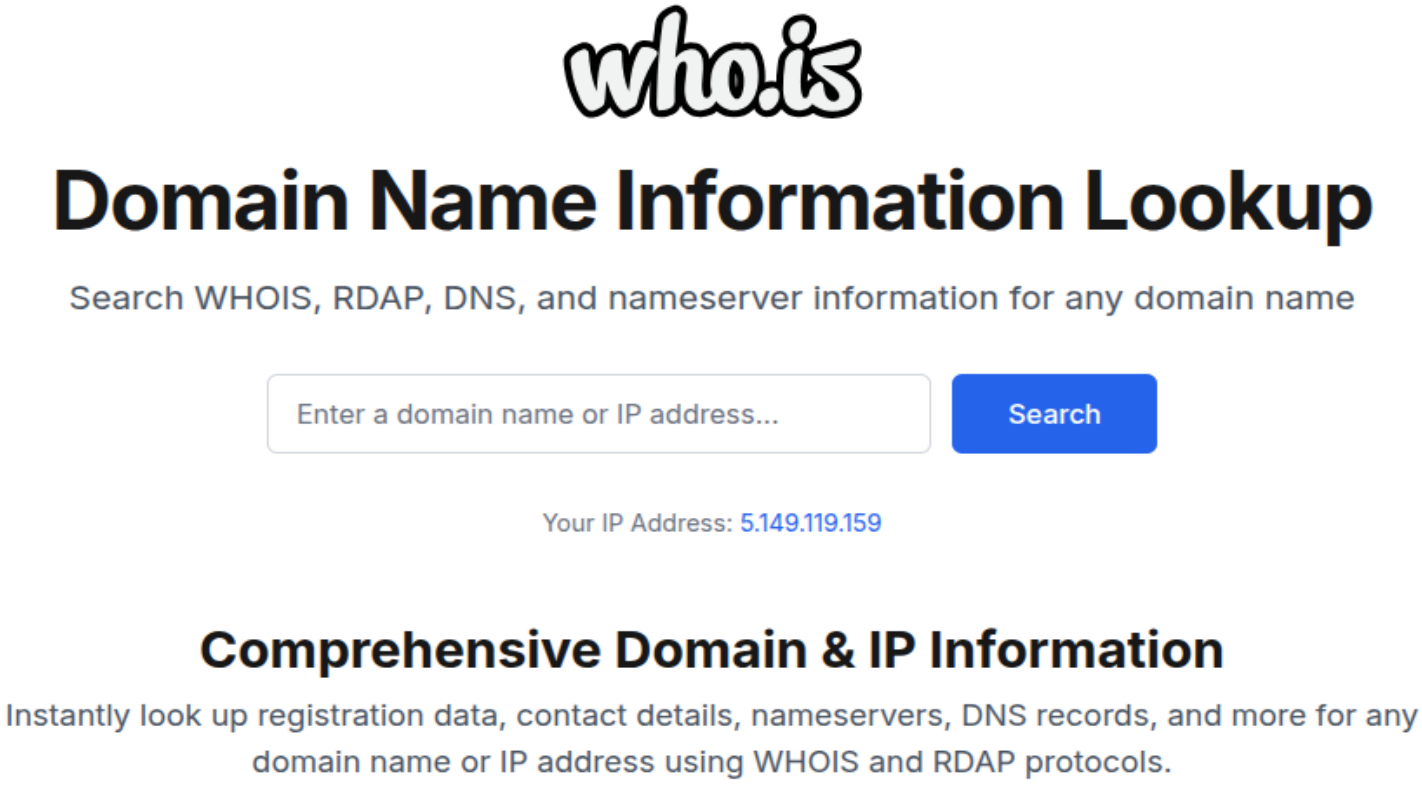
- https://www.filescan.io/


Filescan.io
Community
REPORTS
TRENDS
HUNTING
LEADERBOARD
API
FEED
BLOG
EN
SIGN IN
Welcome to the Filescan.io Community!
Uncover Hidden Threats: Insightful Malware Analysis Powered by Emulation
The local threat graph has 73M+ IOCs and MD Cloud Reputation is adding 40B+ Hashes, IPs, Domains for maximum protection.
ANALYZE FILE/URL
THREAT HUNTING
Copy paste your URL
http://www.webpage.com/invoice.doc
Analyze Link
Drag & Drop your File
Max. file size is 100MB
The free community version of Filescan.io is powered by MetaDefender Sandbox that operates 10 times faster than traditional sandboxes and uses 90% fewer resources. It uses adaptive threat analysis technology to detect evasive malware and extract relevant Indicators of Compromise (IOCs). Our threat-agnostic scanning supports a wide variety of files and URLs to identify IOCs swiftly and efficiently.
Learn more

Suspicious Email Analysis

Domain and WHOIS Lookup

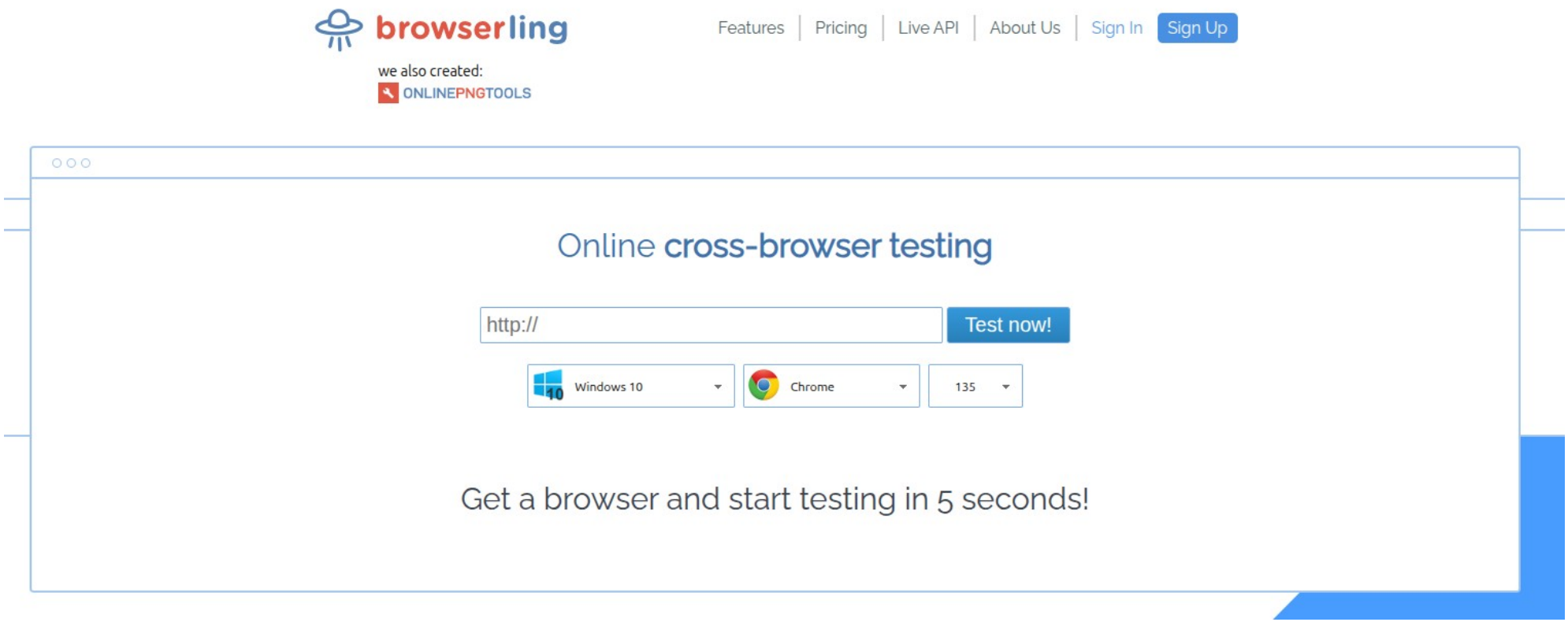
- https://who.is


who.is
Domain Name Information Lookup
Search WHOIS, RDAP, DNS, and nameserver information for any domain name
Enter a domain name or IP address...
Search
Your IP Address: 5.149.119.159
Comprehensive Domain & IP Information
Instantly look up registration data, contact details, nameservers, DNS records, and more for any domain name or IP address using WHOIS and RDAP protocols.

Suspicious Email Analysis

Website Preview

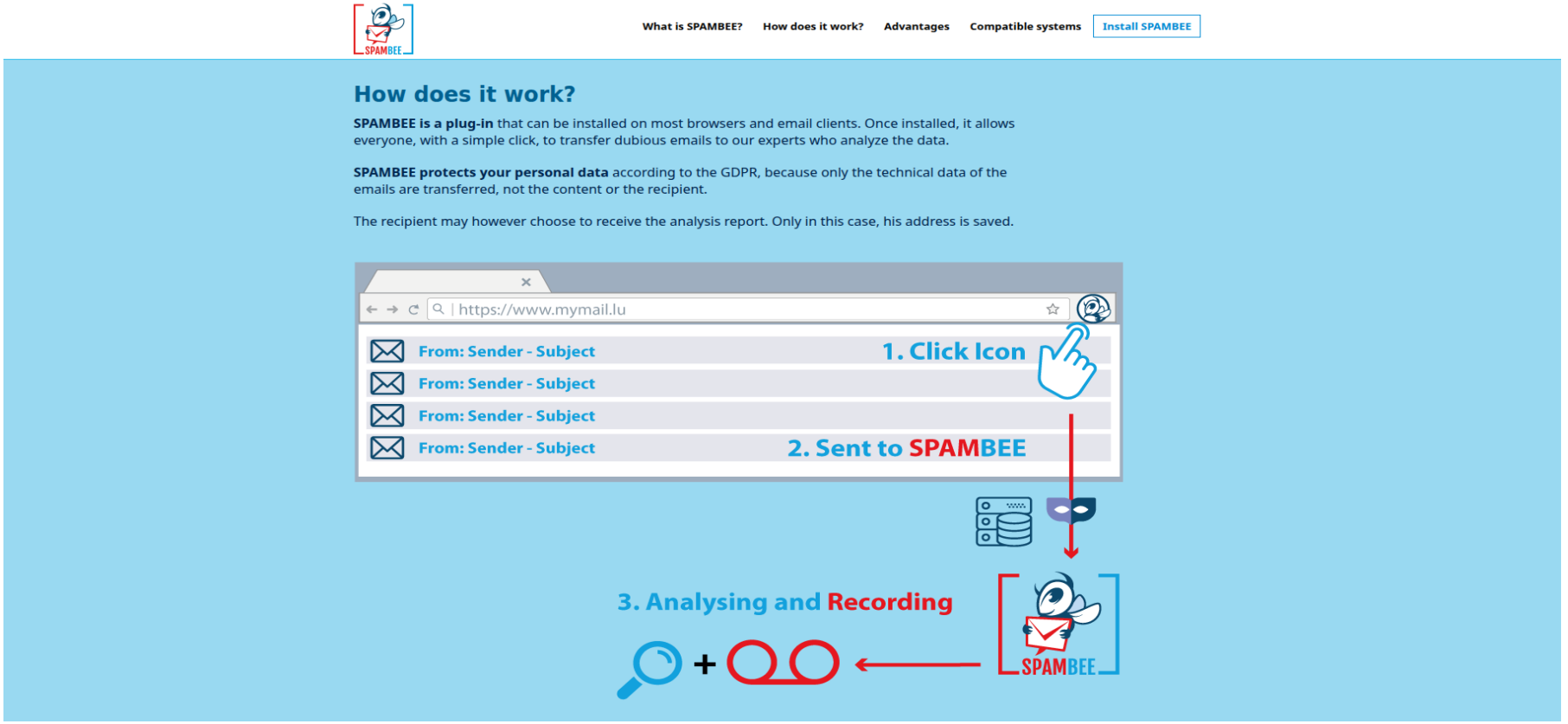
- https://www.browserling.com/



Reporting

Report Phishing Email

- https://spambee.lu/


What is SPAMBEE?
How does it work?
Advantages
Compatible systems
Install SPAMBEE
How does it work?
SPAMBEE is a plug-in that can be installed on most browsers and email clients. Once installed, it allows everyone, with a simple click, to transfer dubious emails to our experts who analyze the data.
SPAMBEE protects your personal data according to the GDPR, because only the technical data of the emails are transferred, not the content or the recipient.
The recipient may however choose to receive the analysis report. Only in this case, his address is saved.
https://www.mymail.lu
From: Sender - Subject
From: Sender - Subject
From: Sender - Subject
From: Sender - Subject
1. Click Icon
2. Sent to SPAMBEE
3. Analysing and Recording
SPAMBEE

CIRCL Tools

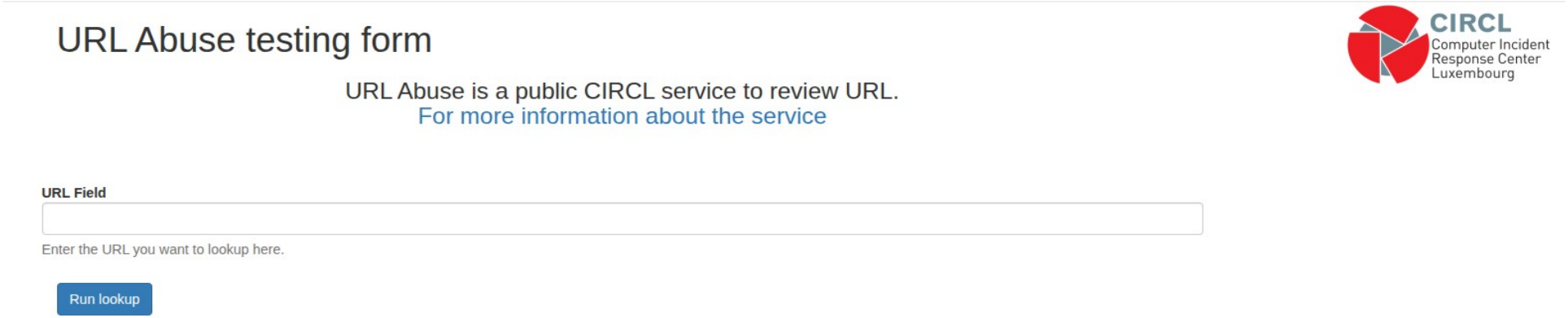
Who is CIRCL ?

CIRCL, or the **C**omputer **I**ncident **R**esponse **C**enter **L**uxembourg, is the national **C**ERT (**C**omputer **E**mergency **R**esponse **T**eam) for the private sector, communes, and non-governmental entities in Luxembourg

CIRCL Tools

CIRCL URL Abuse

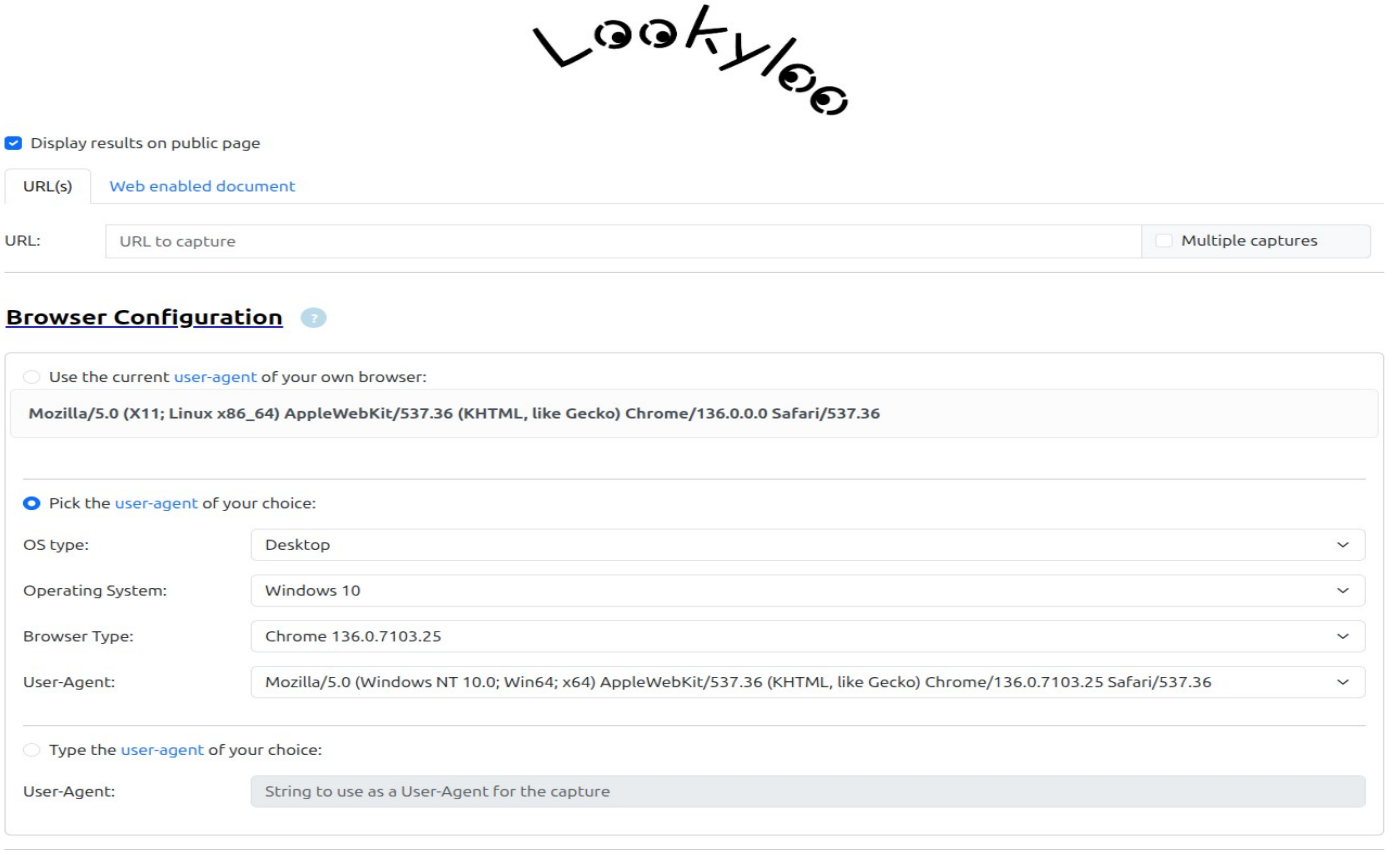
- https://www.circl.lu/urlabuse/



CIRCL Tools

Lookyloo

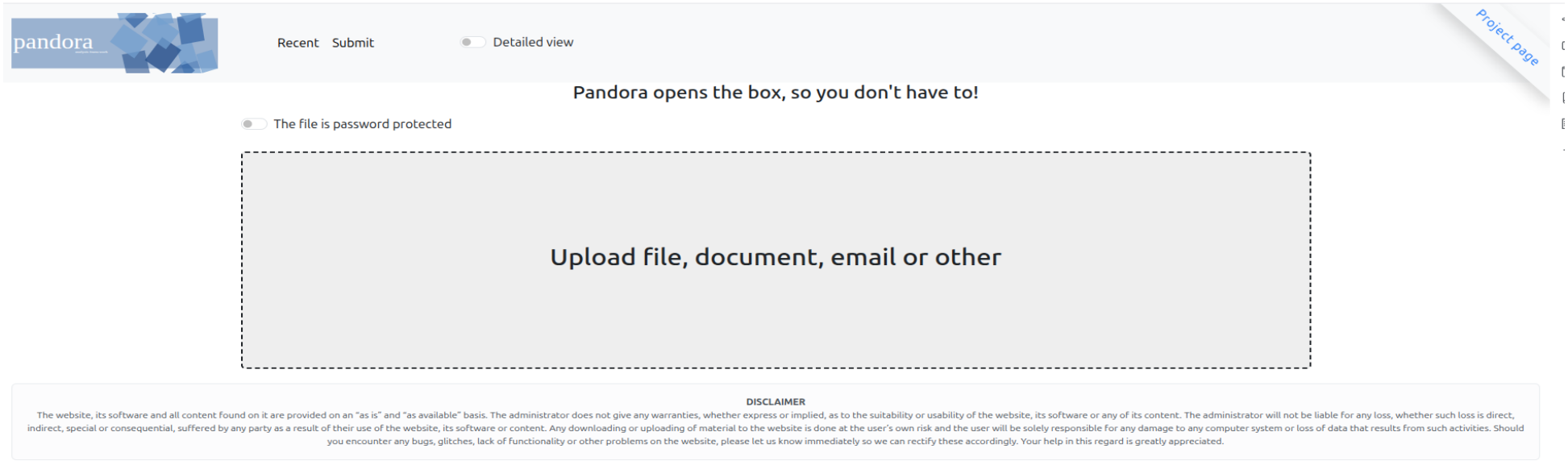
- https://lookyloo.circl.lu/



CIRCL Tools

Pandora

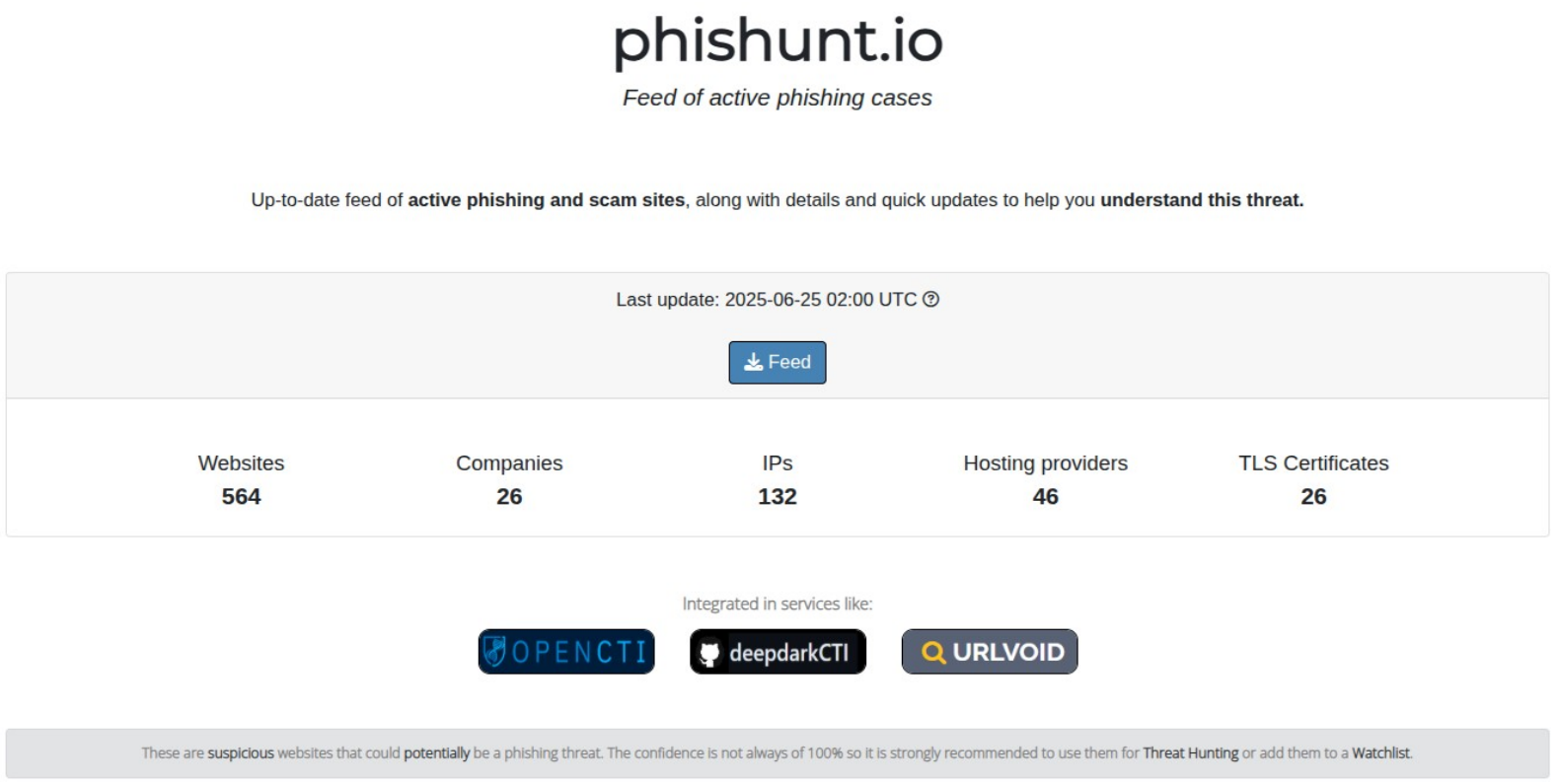
- https://pandora.circl.lu/


pandora
Recent
Submit
Detailed view
Project page
Pandora opens the box, so you don't have to!
The file is password protected
Upload file, document, email or other
DISCLAIMER
The website, its software and all content found on it are provided on an "as is" and "as available" basis. The administrator does not give any warranties, whether express or implied, as to the suitability or usability of the website, its software or any of its content. The administrator will not be liable for any loss, whether such loss is direct, indirect, special or consequential, suffered by any party as a result of their use of the website, its software or content. Any downloading or uploading of material to the website is done at the user's own risk and the user will be solely responsible for any damage to any computer system or loss of data that results from such activities. Should you encounter any bugs, glitches, lack of functionality or other problems on the website, please let us know immediately so we can rectify these accordingly. Your help in this regard is greatly appreciated.

Reported Domains

Blacklists and Reported Domains

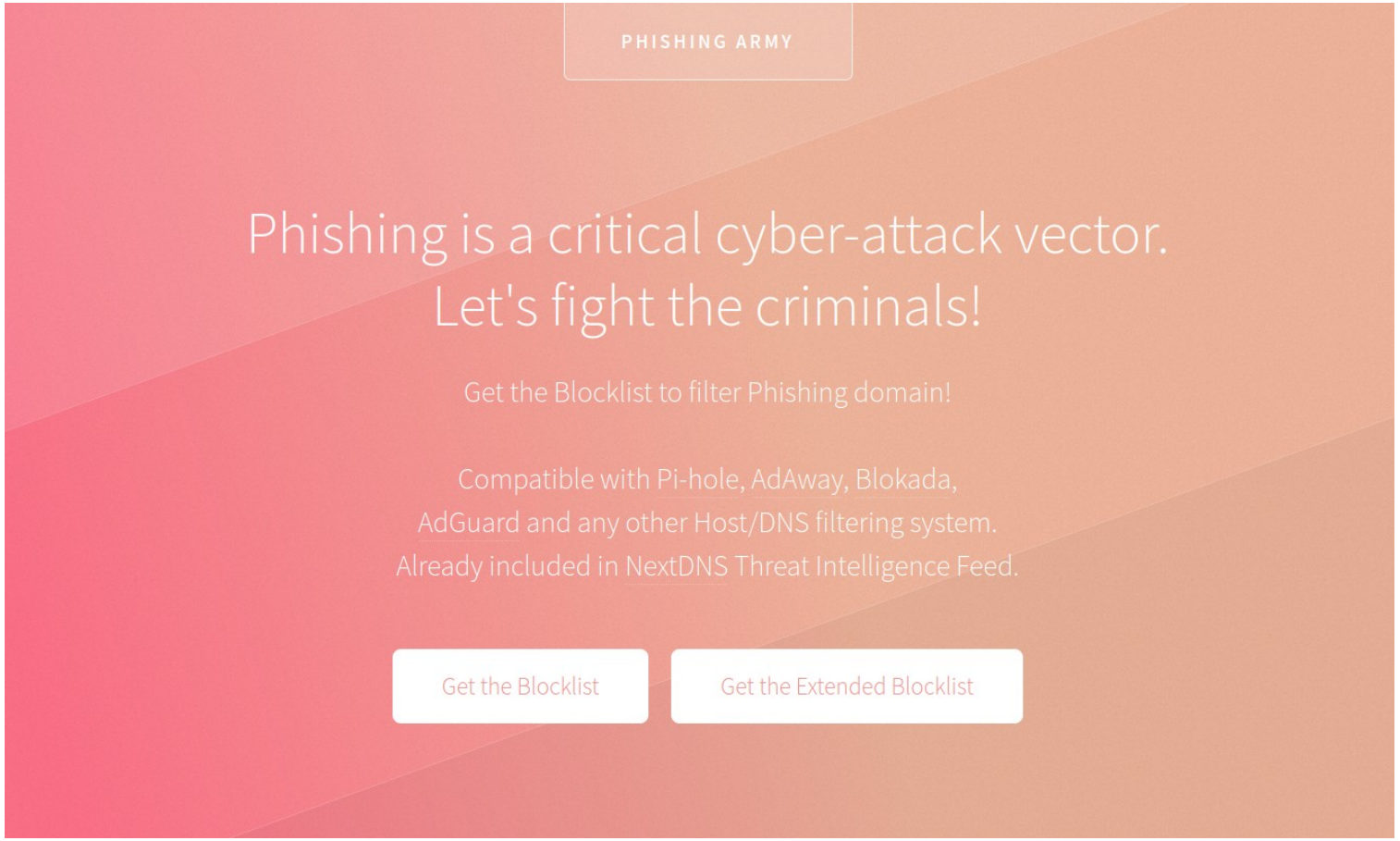
- PhishHunt: https://phishunt.io/


phishunt.io
Feed of active phishing cases
Up-to-date feed of active phishing and scam sites, along with details and quick updates to help you understand this threat.
Last update: 2025-06-25 02:00 UTC
Feed
Websites
564
Companies
26
IPs
132
Hosting providers
46
TLS Certificates
26
Integrated in services like:
OPENCTI
deepdarkCTI
URLVOID
These are suspicious websites that could potentially be a phishing threat. The confidence is not always of 100% so it is strongly recommended to use them for Threat Hunting or add them to a Watchlist.

Reported Domains

Blacklists and Reported Domains

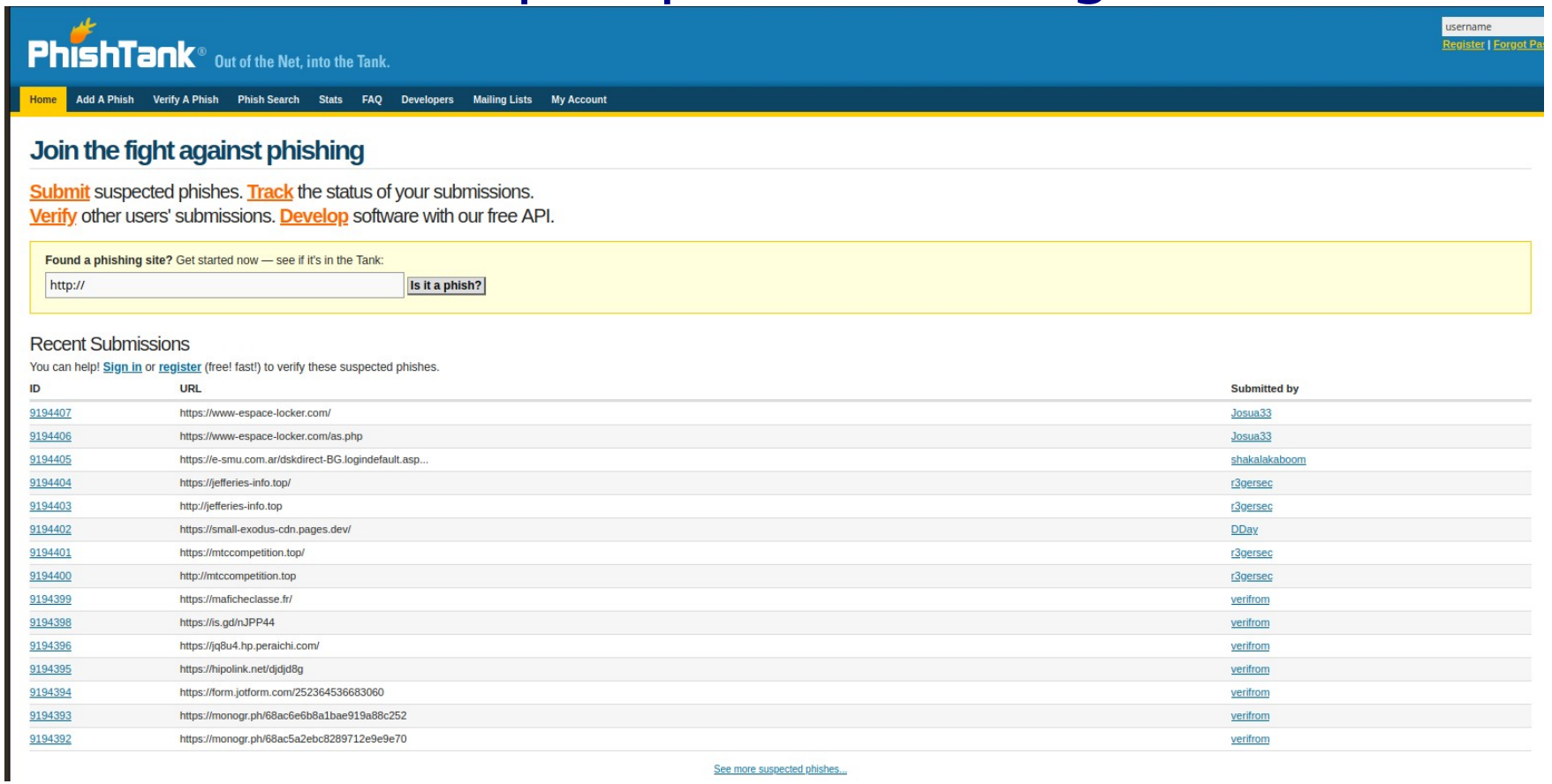
- Phishing Army: https://phishing.army/


PHISHING ARMY
Phishing is a critical cyber-attack vector.
Let's fight the criminals!
Get the Blocklist to filter Phishing domain!
Compatible with Pi-hole, AdAway, Blokada,
AdGuard and any other Host/DNS filtering system.
Already included in NextDNS Threat Intelligence Feed.
Get the Blocklist
Get the Extended Blocklist

Reported Domains

Blacklists and Reported Domains

- PhishTank: https://phishtank.org/



PhishTank® Out of the Net, into the Tank.

username
Register | Forgot Pa

Home | Add A Phish | Verify A Phish | Phish Search | Stats | FAQ | Developers | Mailing Lists | My Account

Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

http:// Is it a phish?

Recent Submissions

You can help! Sign in or register (free! fast!) to verify these suspected phishes.

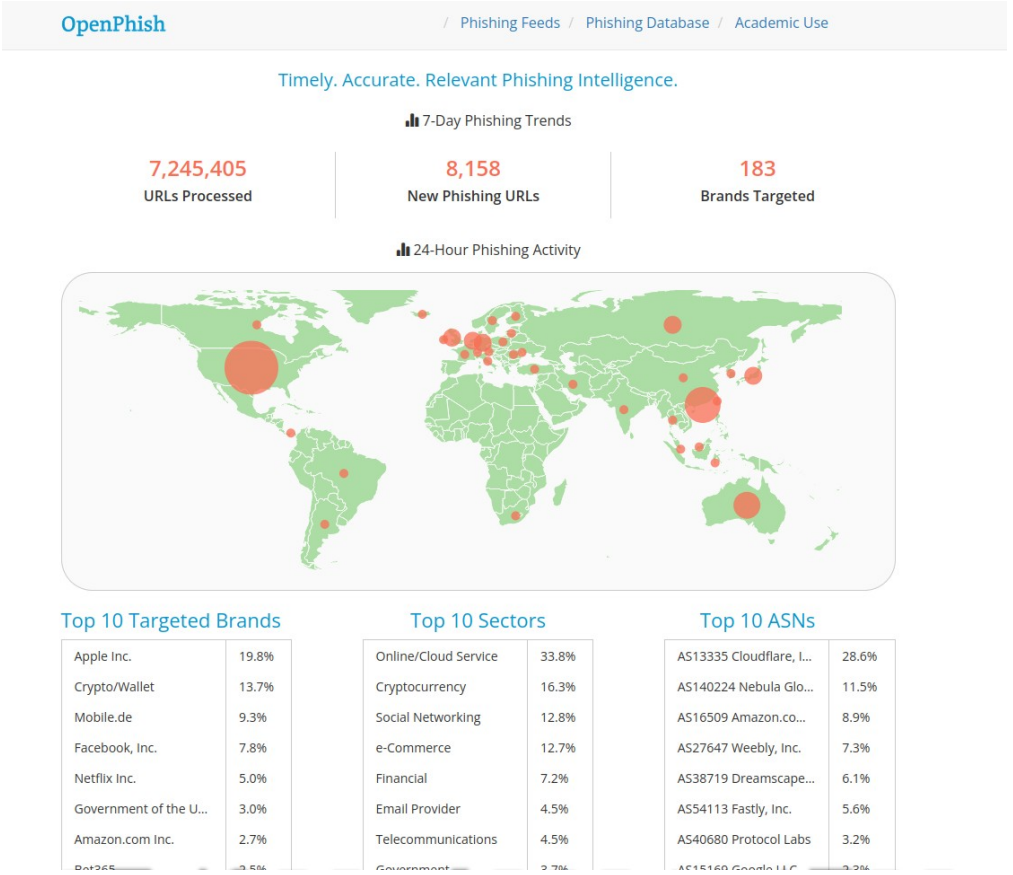
ID	URL	Submitted by
9194407	https://www-espace-locker.com/	Josua33
9194406	https://www-espace-locker.com/as.php	Josua33
9194405	https://e-smu.com.ar/dskdirect-BG.logindefault.asp...	shakalakaboom
9194404	https://jefferies-info.top/	r3gersec
9194403	http://jefferies-info.top	r3gersec
9194402	https://small-exodus-cdn.pages.dev/	DDay
9194401	https://mtccompetition.top/	r3gersec
9194400	http://mtccompetition.top	r3gersec
9194399	https://maficheclasse.fr/	verifrom
9194398	https://is.gd/nJPP44	verifrom
9194396	https://jq8u4.hp.peraichi.com/	verifrom
9194395	https://hipolink.net/djdjd8g	verifrom
9194394	https://form.jotform.com/252364536683060	verifrom
9194393	https://monogr.ph/68ac6e6b8a1bae919a88c252	verifrom
9194392	https://monogr.ph/68ac5a2ebc8289712e9e9e70	verifrom

See more suspected phishes...

Realtime Statistics

OpenPhish

- https://openphish.com/



Phishing Attacks

Thank you